Abstract of the Disclosure

A security system for securing an entity or a service from indiscriminate access and a method for operating the same is disclosed. Each designated person of M designated persons is provided with a portable biometric device. Biometric data in dependence upon a biometric characteristic of each of the M designated persons is stored in memory of the respective portable biometric device. Biometric information representative of a biometric characteristic of each of a subset of $1 < N < M$ persons is captured in response to each of the N persons presenting said information to the respective portable biometric device. The biometric information is encoded and biometric data in dependence thereupon is provided to the processor of each respective portable biometric device. Using the processor of each respective portable biometric device the captured biometric data is then compared with the stored biometric data to produce a comparison result. If the comparison result is indicative of a match an authorization signal is transmitted from each of the respective portable biometric devices to a receiving port of the security system. Upon receipt of the authorization signal a processor of the locking mechanism determines access privileges to the secure entity or service in dependence upon the authorization signals it received from the respective portable biometric devices of the subset of N persons. If an authorization signal of the subset of N persons is missing, the security system denies access to the secure entity or service.